POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Ladisa S.r.l. considera come obiettivo primario la sicurezza delle informazioni. Questo significa implementare e mantenere un sistema di gestione delle informazioni sicuro, così da garantire:

1. Riservatezza - informazioni accessibili solamente ai soggetti e/o ai processi debitamente autorizzati;

2. Integrità – salvaguardia della consistenza dell'informazione da modifiche non autorizzate, ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.

3. Disponibilità – facilità di accesso alle informazioni necessarie, ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

4. Controllo - garanzia che i processi e strumenti per la gestione dei dati siano sicuri e testati;

5. Autenticità - provenienza affidabile dell'informazione.

6. Privacy – garanzia di protezione e controllo dei dati personali.

Ladisa S.r.l. ha sviluppato un Sistema di gestione della sicurezza dell'informazione (SGSI), seguendo i requisiti specificati della Norma UNI CEI EN ISO/IEC 27001:2013 e successivi corrigendum.

Il patrimonio informativo della Ladisa S.r.l. da tutelare è costituito dall'insieme delle informazioni localizzate nella sede dell'azienda.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

☐ Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

☐ Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.

☐ Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.

☐ Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.

☐ Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.

☐ È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.

☐ Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.

☐ Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.

☐ Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

☐ Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'attività di Ladisa S.r.l., la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine aziendale.

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Gli obiettivi generali di Ladisa S.r.l. sono quindi:

• garantire i migliori standard, ottimizzando e razionalizzando i processi e gli strumenti aziendali;

• garantire l'efficacia del SGSI;

• garantire la soddisfazione degli utenti in relazione alla qualità delle informazioni.

Tutto il personale deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni. L'applicazione del sistema di gestione richiede pertanto piena partecipazione, impegno ed efficace interazione di tutte le risorse umane e tecnologiche. La continua crescita del livello di servizio verrà perseguita mediante il regolare riesame dello stesso, volto al monitoraggio degli obiettivi prestabiliti e al riconoscimento di eventuali aree di miglioramento.

La Direzione è impegnata per:

1) attuare, sostenere e verificare periodicamente la presente Politica, a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa;

2) garantire le risorse necessarie per l'efficace protezione delle informazioni;

3) definire gli obiettivi in materia di sicurezza delle informazioni;

4) riesaminare periodicamente gli obiettivi e la Politica per la sicurezza delle informazioni per accertarne la continua idoneità.

Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.

Data, 22.02.2023

Direzione